DETERRING NETWORK INCURSION

Mark L. Wilkinson
Ronald J. Miller
Michael J. McDaniels

5

ABSTRACT OF THE DISCLOSURE

A system, method, and computer-readable medium for deterring network incursion by formulating appropriate responses to attacks. Once an attack is detected, the system may respond in such a manner as to imitate a network device. The system may respond in a

10 manner that provides a high cost to pursue further communication with the system. For example, the system may respond to TCP syn requests and window probes with messages indicating small packet and window sizes. As such, attempts to send packets to the system have a high network and processing cost. An attacking computer running multiple threads may ultimately slow or be disabled as a result of the receiving the responses and attempting

15 to continue to communicate with the system.